

## **SECURITY ADVISORY**

Dolibarr Arbitrary File Upload (Authenticated)

### **BELABED Skander**

16/05/2023 CVE-2023-38887



### **RENNES – PARIS**

Siège social - 37 Boulevard Solférino - 35000 RENNES Tel +33(0)1 53 76 86 35 | E-mail contact@akerva.com



# **Table of contents**

SUMMARY	3
Context	3
Description	3
Products and versions affected	3
Impact	3
Mitigations	3
Disclosure timeline	3
TECHNICAL DETAILS	4
Vulnerability Details	4
Proof of Concept (PoC)	6
Risk Characterization	7
References	7
ABOUT AKERVA	8
Who are we?	8
Join us	8
Contact	8



## SUMMARY Context

Product description:

Dolibarr ERP CRM is an open source, free software package for companies of any size, foundations or freelancers. It includes different features for enterprise resource planning (ERP) and customer relationship management (CRM) but also other features for different activities.

### Description

If both "DMS/ECM" and "REST API" modules are enabled, any authenticated user with the permission of submitting documents can upload arbitrary files using API calls.

### **Products and versions affected**

Affected products:

• Dolibarr 17.0.1 and earlier

### Impact

Possibility of uploading malicious files which sometimes can lead to arbitrary command execution on the hosting server.

### Mitigations

Upgrade to the latest version of the product.

### **Disclosure timeline**

DATE	EVENT
16/05/2023	Initial discovery.
07/07/2023	Initial contact with security@dolibarr.org
21/07/2023	Vulnerability acknowledged by Dolibarr's team
18/08/2023	Fix published by Dolibarr's team
18/09/2023	Public disclosure



## **TECHNICAL DETAILS**

### Vulnerability Details

One of the pre-installed modules in Dolibarr is "DMS/ECM", which in summary, lets the users to manage their documents in an automatic or manual way.

Participanti volce Verticipanti volce Verticipanti volce Verticipanti volce     Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: volce   Image: vo	$\leftarrow \rightarrow \mathbf{G}$	O 😫 192.168.1.50/ecm/index_auto.php								습	🗢 🤻 🍯 😤 ව
Search       Manual tee @         Lobascia       Manual tee @         Lobascia       C         Disconie       Documens       Size       Date         Bark acconit       0       Select à dilectory in the tree       Select à dilectory in the tree         Contracts       0       Select à dilectory in the tree       Select à dilectory in the tree         Contracts       0       Select à dilectory in the tree       Selectory       Selectory         Contracts       0       Selectory       Selectory       Selectory       Selectory         Contracts       0       Selectory       Selectory       Selectory       Selectory         Selectory       0       Selectory       Selectory       Selectory       Selectory         Selectory       0       Selectory       Selectory       Selectory       Selectory         Selectory       0       Selectory       Selectory       Selectory       Selectory       Selectory         Selectory       0       Selectory       0       Selectory       Selectory       Selectory       Selectory         Selectory       0       Selectory       0       Selectory       Selectory       Selectory       Selectory       Selectory<					HRM Docum	ents Agenda		les			🗚 🖯 🖸 17.0.1 🔺 🌘
Image: Second	search 👻	Manual tree 💿 Automatic tree 💿			1						
Detectories         Documents         Size         Date                3 Bank accourt             4 Condidaures               Selecta directory in the tree               Selecta directory in the tree               Selecta directory in the tree                 2 Condradiatures               Contracts               Selecta directory in the tree               Selecta directory in the tree                 2 Contracts             Contreton             Contract	lanual tree	C									
2       I dui Notodia         4       Condidataria         6       Contractio         6       Costinici invoices         6       Costinici invoices         1       Products and Services         1       Products and Services         1       Products and Services         1       Salaris	utomatic tree	Directories		Documents					Size	Date	
2 <ul> <li>Check deposit</li> <li>Commercial proposals</li> <li>Commercial proposals</li> <li>Contracts</li> <li>Contracts</li></ul>		Bank account	0	Select a director	y in the tree						
Image: Commonial proposals       Image: Commonial proposals         Image: Commonial proposals       Image: Commonial		Candidatures	0								
Image: Contracts       Image: Contracts         Image: Contrents		ia Check deposit	0								
2       a Gustomer invoices       a         a Gustomer invoices       a         a Expense reports       a         a Interventions       a         a Interventions       a         a Products and Services       a         a Products and Services       a         a Sales orders       a         a Sales Orders       a         a Sales Orders       a         a Sales Orders       a         b Social tracs       a         b Ottops       a         b Social or fiscal taxes       a         b Ottops       a         b Ottops       a         b Ottops       a		Commercial proposals	0								
Image: Expense reports       Image: Ima	-	Contracts	0								
Inferventions       Inferventions         Inferventions	2										
Image: Amulacturing orders     Image: Amulacturing orders       Image: Amulacturing orders		Expense reports									
Products and Services     0       Products and Services     0       Products and Services     0       Salantes     0       Salact Orders     0       Salact States     0											
ProjectsImage: Comparison of the comparis											
I Purchase orders     I       I Salaries     I											
I Salarios     I       I Sales Circlers     I       I Sales tax     I       I Social or fiscal taxes     I       I Taxks     I       I Taxks     I       I Taxks     I       I Users     I											
I Sales Orders     I       I Sales tax     I       I Social or Social taxes     I       I Taxis     I											
Sales tax     Image: Comparison of the sector											
Social or fiscal taxes     Image: Comparison of the second s											
Tasks     0       Third parties     0       Users     0											
Third-parties O Gutters O											
Car Users 0											
		Vendor invoices	0								

#### FIGURE 1: ECM AUTOMATIC TREE VIEW.

In order to avoid an Arbitrary File Upload which sometimes can lead to Arbitrary Command Execution, the application is going to append ".noexe" extension at the end of any file having a "dangerous" extension.

	U 🐴 192.168.1.50/ec	cm/index.php?action=file_manage		leftmenu=ecm&idme				ជ	🗢 🏶 🧕 🚽	ື ີ ≡
Home Third-parties Products		Commerce Billing   Payment Banks	t Q  Cash Accounting	HRM Documents A	箇 🗃	▶ Sols Websites			<b>r 🔒 😗</b> 17.0.1	* 🔔
Search 👻	Manual tree 💿 🛛 A	Automatic tree ()								
DMS/ECM area Manual tree Automatic tree	ta C'					Browse	No files selected.	Over	write file if exists UPLOA	D O
	Directories		▼ Documents		Siz	•	Date			
	😂 test	1 / 0	🕞 test.php		01		05/31/2023 10:36 AM			/=
	ole ⊃ Debugger ↑L N	etwork () Style Editor () Pe	rformance <b>1</b> Me	norv El Storade	Accessibility	Application				ന
Conso	ole 🕞 Debugger ↑↓ Ne	ietwork () Style Editor 🎧 Pe	rformance 10: Me	nory 🗄 Storage	🛉 Accessibility 🏼	Application +	✓ ♥ Filter Styles they cls +	* 0 0	E Layout Compute	
Search HTML	id="tablelines" class=")	etwork () Style Editor က Pe	_	nory 🖹 Storage	🕇 Accessibility 📓		¥ Filter Styles they cls + element ⊞ {			
Conso Co	id="tablelines" class=" y> class="liste_titre nodr Line list of documents	<pre>centpercent liste noborder no rag nodrop"&gt;&gt;==</pre> 0 relativepath = test/>	_	nory 🗄 Storet	🕇 Accessibility 📓		<pre>element ::: { } a:link, a:visited, a:hover, styl a:active, .classlink ::: {</pre>		E Layout Compute	ed Chai
Conso     Cons     Cons     Conso     Conso     Conso     Conso     Conso     Con	id="tablelines" class=" y> class="liste titre nodr	<pre>centpercent liste noborder no rag nodrop*&gt;(m      0 relativepath = test/&gt; 0 -&gt;</pre>	_	nory 🗄 Storage	🕇 Accessibility 📓		<pre>element () { } a:link, a:visited, a:hover, styl</pre>	inline	Layout Compute     Flexbox     Select a Flex container o	d Char
Conso Cost Search HTML Cost	id="tablelines" class=" y> class="liste_titre nodr -line list of documents -In database: position=0 id="row AFTER0POS1" cla d class="miwith200 tdo	<pre>centpercent liste noborder no rag nodrop*&gt;@ 0 relativepath = test/&gt; 0&gt; ass="oddeven*&gt; verflowmax500"&gt;</pre>	bottom">	nory 🗄 Storede	Accessibility	+ 8	<pre>element ::: { } a:link, a:visited, a:hover, styl a:active, .classlink ::: {     color: ● var(colortextlink);     text-decoration: ▶ none; }</pre>	inline le.css.php:112	Layout Compute     Flexbox     Select a Flex container o     continue.	d Char
2, Search HTML	id="tablelines" class=" y> class="liste_titre nodr -line list of documents -In database: position=0 id="row AFTER0POS1" cla d class="miwith200 tdo	"centpercent liste noborder no rag nodrop">(=  0 relativepath = test/>   0-3	bottom">	nory E Storede	Accessibility		<pre>element ::: { } a:link, a:visited, a:hover, styl a:active, .classlink ::: {     color: ● var(colortextlink);     text-decoration: ▶ none; }</pre>	inline	Elayout Compute     Flexbox     Select a Flex container o     continue.     Grid	or item to

FIGURE 2:.NOEXE EXTENSION APPENDED AFTER PHP FILE UPLOAD.

Akerva – Security advisory – Dolibarr – Arbitrary File Upload (Authenticated) CVE-2023-38887



The code responsible for this behavior is the following, which basically before writing the file to the disk, checks if the original file extension matches with one of the blacklisted ones:



FIGURE 3: PART OF DOL\_MOVE\_UPLOADED\_FILE (HTDOCS/CORE/LIB/FILES.LIB.PHP).



#### FIGURE 4: ISAFILEWITHEXECUTABLECONTENT FUNCTION (HTDOCS/CORE/LIB/FUUNCTIONS.LIB.PHP).

Another Dolibarr pre-installed module is "API / WEB SERVICES" which enables a REST server and lets the users do all kinds of actions through API calls. One of these actions is the document upload and after analyzing the related class (htdocs/api/class/api\_documents.class.php), it was noticed that excepting some

sanitizations, no security measures to prevent arbitrary file upload were present.



### **Proof of Concept (PoC)**

Let's assume that both REST API and DMS/ECM modules are enabled in Dolibarr and we have an account which has the permission of submitting data using DMS/ECM module. We just need to get the API key linked to our account and send an authenticated API request containing our malicious file as shown below:

← → C O	8 192.168.1.50/ecm/ind	dex_auto.php?module=pro 🏠	⊚ ± €	🐭 🥕 🦉 👳	മ≣	File Edit Vi	ew Help																																																																																	
* • • • • •					<b>A</b>	Home Wo	orkspaces ~ Explore																																																																																	
	je Comi Billini Bank Acco HRM		1	<b>H 🖯 17.0.1</b>	test1 ~			🖧 Working loca	ally in Scratch Pad. Switch to a	Workspace																																																																														
	🔄 Purchase orde	ers			0	POST logi	• • + •••																																																																																	
	Salaries				0	& test /	lasia			🖺 Save																																																																														
	Sales Orders				0		Ngill																																																																																	
	Sales tax				0	POST	<ul> <li>http://192.168.1.50/api/index</li> </ul>	php/documents/upload	1																																																																															
	Social or fiscal	taxes			0	Darame	Authorization Headers (9) Bod	hr . Dra-ranuast Seriet	Taste Sattings																																																																															
	Tasks				0	1																																																																																		
	Third-parties				0	© non	e 🔘 form-data 🍥 x-www-form-uriend	oded 🐞 raw 👳 binary	GraphQL JSON V																																																																															
	Users				0	1	filename": "shell.php",																																																																																	
	Vendor invoice	es .			0		"modulepart": "project", "ref": "",																																																																																	
							<pre>subdit*: "PJ2305-0001". filecontent*: "PD9waHAgc31zdG</pre>																																																																																	
					Q ×		"fileencoding": "base64",																																																																																	
	≠ Ref.	Documents	Size	Date	Shared		"overwriteifexists": "1", "createdirifnotexists": "1"																																																																																	
	"" PJ2305-0001	🖉 PJ2305-0001.pdf 🔍	6911 b. 05/	26/2023 02:35 PM																																																																																				
	" PJ2305-0001	🗟 sheli.php 🔍	13 b. 05/	31/2023 11:40 AM																																																																																				
👁 Variables Timeline I	Error handler 139 Database	e 🖪 Logs 📧	S Q 2 2	204208 Bytes 18.1	17ms 🔺 🗙																																																																																			
API	~ ~	Highlight All Match Case	Match Diacritic	s 📃 <u>W</u> hole Word	is 2c×	Body				Status: 200 OK Time: 32 ms Size:																																																																														
🕞 🗘 Inspector	Console D Debugger	↑↓ Network {} Style Editor	Performance	» (	б) ••• ×	Pretty																																																																																		
Q, Search HTML			🖋 🗑 Filter [	Layout Co	mputed C		"shell.php*																																																																																	
	Line list_of_au<br <tr <="" class="oddeven" td=""><td><pre>stoecnfiles keg=0&gt; '&gt;m</pre></td><td>:hov .cl</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td>stoecnfiles key+1&gt;</td><td>element</td><td>Select a Flex cont</td><td>ainer or item</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td>&gt; &gt;</td><td>2</td><td>}</td><td>continue.</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td><pre>v  v <td <t<="" <td="" td="" v=""><td>ent.php?modulepart=project&amp;</td><td>a:link,</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></pre></td></tr> <tr><td></td><td>attachment=1&amp;fil</td><td>le=PJ2305-0001%2Fshell.php"</td><td>a:nover</td><td>CSS Grid is not in t</td><td>use on this pa</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td>href="/document</td><td>.php?modulepart=project&amp;</td><td>a:activ '</td><td>* Box Model</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td><pre>mime="text/plain</pre></td><td><u>le=PJ2305-0001%2Fshell.php</u>" n" target="_blank"&gt; event</td><td>1</td><td>margin</td><td>θ</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>div.fiche &gt; div.fiche &gt; div.t</td><td></td><td>&gt; div#ecm-layout-center.inline-block &gt;</td><td></td><td>border</td><td>0</td><td>🐔 🔍 Find ar</td><td>d Replace 🔄 Console</td><td></td><td></td><td></td></tr>	<pre>stoecnfiles keg=0&gt; '&gt;m</pre>	:hov .cl										stoecnfiles key+1>	element	Select a Flex cont	ainer or item							> >	2	}	continue.								<pre>v  v <td <t<="" <td="" td="" v=""><td>ent.php?modulepart=project&amp;</td><td>a:link,</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></pre>	<td>ent.php?modulepart=project&amp;</td> <td>a:link,</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	ent.php?modulepart=project&	a:link,									attachment=1&fil	le=PJ2305-0001%2Fshell.php"	a:nover	CSS Grid is not in t	use on this pa							href="/document	.php?modulepart=project&	a:activ '	* Box Model								<pre>mime="text/plain</pre>	<u>le=PJ2305-0001%2Fshell.php</u> " n" target="_blank"> event	1	margin	θ						div.fiche > div.fiche > div.t		> div#ecm-layout-center.inline-block >		border	0	🐔 🔍 Find ar	d Replace 🔄 Console			
<pre>stoecnfiles keg=0&gt; '&gt;m</pre>	:hov .cl																																																																																							
		stoecnfiles key+1>	element	Select a Flex cont	ainer or item																																																																																			
	> >	2	}	continue.																																																																																				
	<pre>v  v <td <t<="" <td="" td="" v=""><td>ent.php?modulepart=project&amp;</td><td>a:link,</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></pre>	<td>ent.php?modulepart=project&amp;</td> <td>a:link,</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	ent.php?modulepart=project&	a:link,																																																																																				
	attachment=1&fil	le=PJ2305-0001%2Fshell.php"	a:nover	CSS Grid is not in t	use on this pa																																																																																			
	href="/document	.php?modulepart=project&	a:activ '	* Box Model																																																																																				
	<pre>mime="text/plain</pre>	<u>le=PJ2305-0001%2Fshell.php</u> " n" target="_blank"> event	1	margin	θ																																																																																			
div.fiche > div.fiche > div.t		> div#ecm-layout-center.inline-block >		border	0	🐔 🔍 Find ar	d Replace 🔄 Console																																																																																	

FIGURE 5: ARBITRARY FILE UPLOAD STEPS.

In case of Dolibarr environment is not correctly configured and "documents" directory is exposed by the web server, we can reach the uploaded files which means execute a webshell:

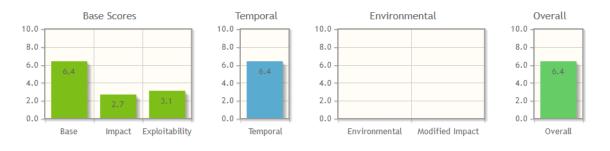


#### FIGURE 6: WEBSHELL EXECUTION.

Another risk is being able to upload malicious executable files that could compromise user security.



### **Risk Characterization**



#### FIGURE 7: CVSS SCORE.

CVSS v3.1 – Base Score			
Attack Vector (AV)	Network (N)	Scope (S)	Changed (U)
Attack Complexity (AC)	Low (L)	Confidentiality (C)	Low (N)
<b>Privileges Required (PR)</b>	Low (L)	Integrity (I)	Low (N)
User Interaction (UI)	None (N)	Availability (A)	None (N)
CVSS v3.1 – Temporal So	core		
Exploit Code Maturity (E)	High (H)		
<b>Remediation Level (RL)</b>	Not Defined (X)		
Report Confidence (RC)	Confirmed (C)		

### References

 Dolibarr, Wikipedia <u>https://www.citethisforme.com/cite/sources/websiteautociteeval</u>



## **ABOUT AKERVA**

### Who are we?

Founded in 2013, *Akerva* is a consulting firm specialized in CyberSecurity and Risk Management. Our *Offensive Technology team (OffTech)* work for our customers to provide them with security assessments through offensive and technical audits in order to identify credible real world compromission scenarios and business risk. Missions such as application or network penetration testing, red team engagements or phishing and social engineering campaigns are complemented by R&D and vulnerability research in our dedicated lab to maintain the highest technical proficiency for our team.

### Join us

Want to be part of the adventure? Join our team of experts by sending your application: <a href="https://akerva.com/jobs/">https://akerva.com/jobs/</a>

### Contact

- Website: <u>https://www.akerva.com</u>
- Blog: <u>https://akerva.com/blog/</u>
- Email: <u>contact@akerva.com</u>
- LinkedIn: <a href="https://fr.linkedin.com/company/akerva">https://fr.linkedin.com/company/akerva</a>
- Twitter: <u>https://twitter.com/Akerva\_FR</u>